

REMARKS

Claims 1-30 are pending in the present application. Claims 1, 4, 7, 8, 11, 13, 14, 17-21, 24, 27 and 28 were amended; and claims 2, 5, 6, 12, 15, 16, 22, 25, and 26 were cancelled. Reconsideration of the claims is respectfully requested.

An amendment was made to the specification to correct an error of a typographical nature. No new matter has been added by the amendment to the specification.

Claims 1, 11, and 21 were amended to better clarify that encryption of a data chunk and calculation of an associated intermediate digital digest from the encrypted data chunk is repeated such that the data package comprises a plurality of encrypted data chunks and associated intermediate digital digests (See Page 11, Lines 9-13, Lines 20-29; and Page 12, Lines 2-5). No new matter has been introduced by the amendments to claims 1, 11, and 21.

Claims 4, 14, and 24 have been amended to better clarify that the claimed decryption method, apparatus, and computer program product decrypt a data package comprising a plurality of encrypted data portions each corresponding to one of a plurality of encrypted intermediate digital digests. (See Figure 6, elements 541-545; Figure 8, steps 810, 830, and 870; Page 4, Lines 10-19; Page 11, Line 25-Page 12, Line 5; and Page 14, Lines 6-28.) No new matter has been introduced by the amendments to claims 4, 14, and 24.

Claims 7, 17, and 27 have been amended to claim the mechanism of discarding the encrypted data package when a mis-match occurs between the decrypted intermediate digital digest and the calculated digital digest (See Page 12, Lines 20-23). No new matter has been introduced by the amendments to claims 7, 17, and 27.

Claims 8, 18, and 28 have been amended to provide proper antecedent basis to amended parent claims 4, 14, and 24. No new matter has been introduced by the amendments to claims 8, 18, and 28.

Also, applicants have submitted proposed corrections to drawings labeled Figure 6 in red ink. The proposed corrections are to correct missing reference numerals 610, 620, 630, and 640 (See subject application, Page 12, Lines 13-26 regarding encrypted data portion 610, calculated digital digest 620, decrypted intermediate digital digest 630,

and next encrypted data portion 640). No new matter is introduced by the proposed corrections to Figure 6. These changes will be incorporated into a formal set of drawings upon approval of the proposed changes by the examiner.

I. 35 U.S.C. § 102, Anticipation

The examiner has rejected claims 1-30¹ under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 4,654,480 to Weiss (hereinafter Weiss). This rejection is respectfully traversed.

With respect to this rejection, a prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218, U.S.P.Q. 781 (Fed. Cir. 1983). In this particular case, each and every feature of the presently claimed invention is not identically shown or described in *Weiss*, arranged as they are in the claims.

For example, amended claim 1 recites the following:

1. A computer-implemented method of encrypting data, the data being comprised of a plurality of data chunks, comprising:
 - encrypting a first data chunk;
 - calculating an intermediate digital digests for the first encrypted data chunk;
 - repeating the encrypting and calculating steps for each data chunk of the plurality of data chunks, thereby creating a plurality of encrypted data chunks and associated intermediate digital digests; and
 - formulating a data package comprising the encrypted data chunks and the plurality of intermediate digital digests.

With regard to claim 1, the Office Action states the following:

¹ The Office Action declares a rejection of claims 1-3, 11-13, and 21-23 (See Office Action dated 9/21/2004, page 2) under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 4,654,480 to Weiss. However, arguments for rejections of claims 1-30 in view of Weiss are set form in the detailed action (See Office Action dated 9/21/2004, Pages 2-4).

As per claims 1, 11, and 21, Weiss teaches encrypting each of the plurality of data chunks; calculating a plurality of intermediate digital digests based on the encrypted data chunks, each intermediate digital digest being associated with one or more of the data chunks; and formulating a data package comprising the encrypted data chunks and the plurality of intermediate digital digests (col. 4, line 63-col. 5, line 20).
Office Action dated 9/21/2004, page 2.

Applicants respectfully disagree. For example, the passage of Weiss cited in the rejection of claim 1 recites the following:

The foregoing problems are solved and the foregoing objects are achieved in one illustrative embodiment of the invention in which apparatus for transmitting or storing encrypted data breaks the data into blocks and *appends to each data block* an error detection code which is calculated from the encrypted data block plus a unique sequence number. The sequence number is generated by a local counter and may be the number of bits, bauds, or characters transmitted and received since a previous resynchronization. The error correcting code is transmitted or stored *with the associated encrypted data block*, but although the sequence number is appended to the data for error code calculation purposes, it is not actually transmitted or stored with the encrypted data and error correcting code. When the encrypted data is retrieved or received, the receiving apparatus appends to each received data block a sequence number derived from a local counter which is synchronized to the counter at the transmitting or storing apparatus and a new error detecting code is calculated for comparison to the error detecting code received or retrieved with the encrypted data. A mismatch between the error detecting codes indicates a transmission or synchronization error. In either case the data can be retransmitted. (*emphasis added*).
Weiss, Column 4, Line 63-Column 5, Line 20

Thus, Weiss explicitly describes a mechanism in which an error detection code is calculated from an "encrypted data block" and that "appends to each data block" the error detection code calculated therefrom. Weiss provides no description or suggestion for repeating encrypting and calculating steps "for each data chunk of the plurality of data chunks" for creating a "plurality of encrypted data chunks and associated intermediate digital digests," nor does Weiss describe or suggest "formulating a data package comprising the encrypted data chunks and the plurality of intermediate digital digests." Rather, Weiss clearly describes a mechanism in which an encrypted data block is appended with a error detection code, or digital digest, derived therefrom and in which the encrypted data block is transmitted with the error detection code appended. That is, in the system described by Weiss, the encrypted data block and appended error detection code

derived therefrom comprise a data package, and as such, no data package comprising the plurality of "encrypted data chunks" and "the plurality of intermediate digital digests" calculated from the encrypted data chunks is described or suggested by Weiss.

For example, Weiss recites the following:

A cyclical redundancy code (CRC) which is a common *error-detecting code is computed for each data block* using both the encrypted data for that block and the sequence number which is appended to the encrypted data. The *encrypted data and its associated CRC are then sent* to the receiving station or stored. (*emphasis added*).

Weiss, Column 5, Lines 22-29.

Thus, Weiss clearly describes a system that calculates an error detecting code for each data block and that sends the encrypted block and the error detecting code calculated therefrom as a single data unit, or data package. Weiss in no manner describes, suggests, or otherwise alludes to calculating a plurality of intermediate digital digests based on each of the plurality of data chunks and "formulating a data package comprising the encrypted data chunks and the plurality of intermediate digital digests."

Moreover, Figure 3 of Weiss shows the following:

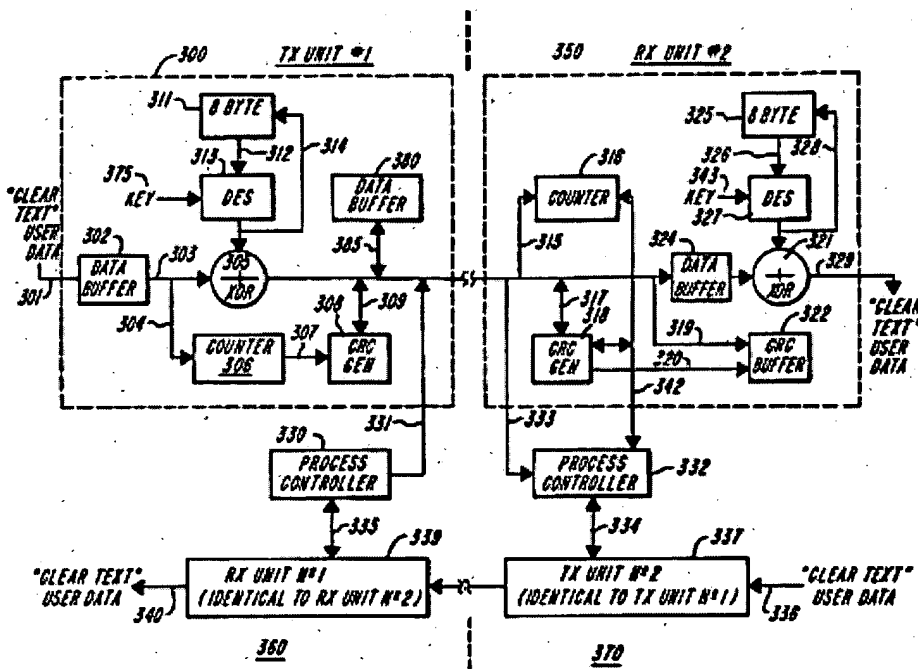


FIG. 3

As can be seen, clear text data (301) is supplied to a buffer (302). The data is divided into blocks at the buffer (Weiss, Column 8, Lines 59-62). Output of an algorithm circuit (313), encrypted key (375), register (311) and feedback paths (312 and 314) is exclusive OR-ed by a gate (305) with the data blocks at the buffer to form encrypted cipher text (See Weiss, Column 8, Line 58-Column 9, Line 3). As each bit of the block is sent to the receiver side (unit 370), the bits of the block are also passed to a generator (308) for calculating an error detecting code, e.g., a cyclic redundancy code (CRC). Weiss clearly describes calculation of the error detecting code as completed after all bits of the block have been passed to the CRC circuit, i.e., generator 308. For example, Weiss states the following regarding calculation of the error detecting code:

As each bit is sent over line 310 to unit 370, it is also provided, via line 309 to cyclic redundancy code generator 308.

Generator 308 is a conventional device which accepts incoming data bits (in this case the encrypted cipher text bits) and generates a CRC which can be used to detect errors in transmission. The complete CRC is a multi-bit code that is generated by circuit 308 *after all data bits* have been passed to the CRC circuit. (*emphasis added*).

Weiss, Column 9, Lines 55-63

When the *final character* of the message has been encrypted, and passed through CRC generator 308, the count in counter 306 which is now equal to the character count in the message (plus the character counts for all previous messages, if any, transmitted since the last resynchronization of the transmitter and receiver) is passed as a multi-bit digital code, via line 307, to CRC generator 308.

Weiss, Column 10, Lines 6-14

After the *last count bit* has been processed by the CRC circuit 308, the *computed CRC* is then passed via line 309 to data transmission facility 310 where the *CRC code bits are treated as additional characters in the message* being sent.

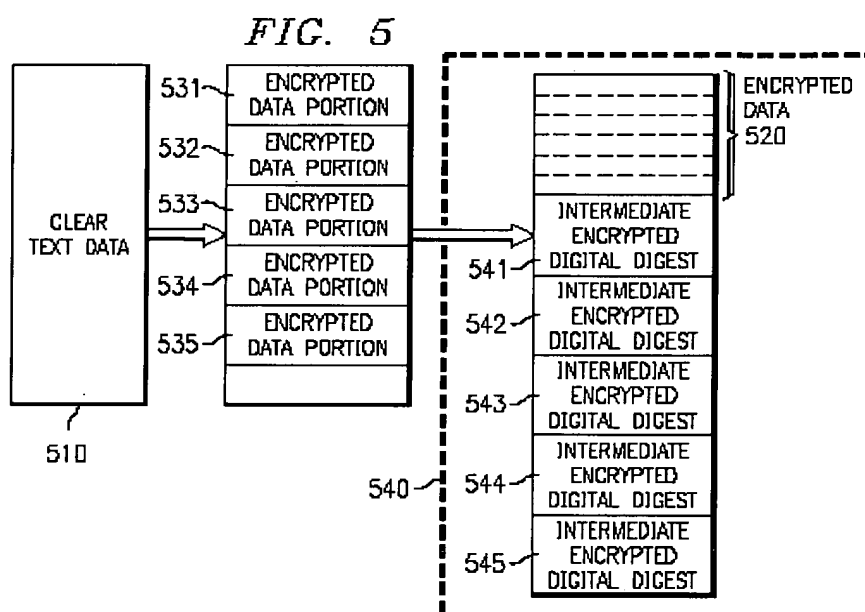
Weiss, Column 10, Lines 20-24

Thus, Weiss is unambiguous that a CRC calculated from an encrypted data block or message is appended to the message and transmitted therewith. (See, for example, Column 8, Line 60-62 and Column 9, Lines 4-6 for equivalence of the terms "message" and "block" as used by Weiss).

Thus, Weiss fails to describe, suggest, or otherwise allude to a method of encrypting data comprising a plurality of data chunks that includes "formulating a data

package comprising the encrypted data chunks" and a "plurality of intermediate digital digests" each calculated and associated with one of the data chunks.

As described in the present application, a method for encrypting each of a plurality of data chunks and calculating a plurality of intermediate digital digests based on the encrypted data chunks is provided. A data package is formulated that comprises the encrypted data chunks and the plurality of intermediate digital digests. For example, Figure 5 of the subject application shows the following:



As can be seen, clear text data (510) is read in "chunks" and encrypted as a plurality of encrypted data portions (531-535). For each encrypted data portion, an intermediate digital digest is generated (541-545). Thus, a plurality of digital digests is generated. The encrypted data portions and corresponding intermediate encrypted digital digests are then used to formulate a data message or packet (540) (See subject application, Page 11, Lines 9-13, Lines 20-21, and Line 25-Page 12, Line 5; Page 13, Lines 16-18, Lines 20-22, and Line 27-Page 14, Line 1; and Figure 7, steps 710-740).

Amended independent claims 11 and 21 recite similar features as claim 1 and were rejected with the same rationale applied to claim 1. Therefore, the same distinctions between Weiss and the claimed invention in claim 1 apply for these claims. For the reasons described above, Weiss does not contain all elements of independent claims 1,

11, and 21. Hence, Weiss fails to anticipate the present invention as recited in claims 1, 11, and 21. Consequently, it is respectfully urged that the rejection of claims 1, 11, and 21 under 35 U.S.C. § 102(b) in view of Weiss has been overcome.

Since claim 3 depends from claim 1, claim 13 depends from claim 11, and claim 23 depends from claim 21, the same distinctions between Weiss and the claimed invention in claims 1, 11, and 20 apply for these claims. Additionally, claims 3, 13, and 23 claim other additional combinations of features not suggested by the reference. Consequently, it is respectfully urged that the rejection of claims 1, 3, 11, 13, 21, and 23 have been overcome.

Therefore, the rejection of claims 1, 3, 11, 13, 21, and 23 under 35 U.S.C. § 102(b) in view of Weiss has been overcome, and such a notice is respectfully requested.

With regard to claim 4, the Office Action states the following:

As per claims 4, 14, and 24, Weiss teaches the encrypted data package being comprised of a plurality of encrypted data portions, comprising: reading an encrypted data portion from the plurality of encrypted data portions; calculating a calculated digital digest for the encrypted data portion; decrypting an intermediate digital digest from the encrypted data package; and authenticating the encrypted data portion based on a comparison of the intermediate digital digest to the calculated digital digest col. 4, line 63-col. 5, lines 63.

Office Action dated 9/21/2004, page 3.

Applicants respectfully disagree. For example, amended claim 4 of the subject application recites the following:

4. A computer-implemented method of decrypting an encrypted data package, the encrypted data package being comprised of a plurality of encrypted data portions and a plurality of encrypted intermediate digital digests, wherein each encrypted data portion corresponds to an encrypted intermediate digital digest, comprising:

reading an encrypted data portion from the plurality of encrypted data portions;

calculating a digital digest for the encrypted data portion;

decrypting an intermediate digital digest corresponding to the encrypted data portion from the plurality of intermediate digital digests;

authenticating the encrypted data portion based on a comparison of the decrypted intermediate digital digest to the calculated digital digest; and

in response to a match, decrypting the encrypted data portion and repeating the reading, calculating, decrypting and authenticating steps for a next encrypted data portion of the data package.

The passage of Weiss cited as teaching the method steps of claim 4 reads as follows:

The foregoing problems are solved and the foregoing objects are achieved in one illustrative embodiment of the invention in which apparatus for transmitting or storing encrypted data breaks the data into blocks and *appends to each data block* an error detection code which is calculated from the encrypted data block plus a unique sequence number. The sequence number is generated by a local counter and may be the number of bits, bauds, or characters transmitted and received since a previous resynchronization. The error correcting code is transmitted or stored *with the associated encrypted data block*, but although the sequence number is appended to the data for error code calculation purposes, it is not actually transmitted or stored with the encrypted data and error correcting code. When the encrypted data is retrieved or received, the receiving apparatus appends to each received data block a sequence number derived from a local counter which is synchronized to the counter at the transmitting or storing apparatus and a new error detecting code is calculated for comparison to the error detecting code received or retrieved with the encrypted data. A mismatch between the error detecting codes indicates a transmission or synchronization error. In either case the data can be retransmitted.

More particularly, in accordance with the invention, the basic method of encryption is the Output Feedback technique and the *data is encoded in blocks*. A cyclical redundancy code (CRC) which is a common *error-detecting code is computed for each data block* using both the encrypted data for that block and the sequence number which is appended to the encrypted data. The *encrypted data and its associated CRC* are then sent to the receiving station or stored. The retrieval or receiving apparatus appends to the encrypted data blocks a sequence number derived from a local counter which is synchronized to the counter at the transmitting or storing apparatus and a new error detecting code is calculated for comparison to the *error detecting code received or retrieved with the encrypted data block*.

Specifically, if the *CRC received with, or retrieved with, a data block* does not match the *CRC computed over that data block* and the sequence number generated the by local counter, then the received data block was either damaged in transmission, or the count in the receiver's local counter doesn't match the transmitter counter count.

In this case, the newly-computed CRC and the received or retrieved CRC are both temporarily stored in a buffer memory, and the receiving unit returns a re-transmission request to the transmitting unit in plain text form. The data is retransmitted in encrypted form along with a CRC computed as previously described. When the retransmitted data block is received, a new CRC code is computed and the newly-computed CRC code is compared to the CRC code received with the re-transmitted data. If a mismatch exists, then the newly-computed CRC code is compared to the CRC codes which were computed for previous transmissions and stored in the CRC buffer memory. If the newly-computed CRC matches one of the stored computed CRCs, then the CRC

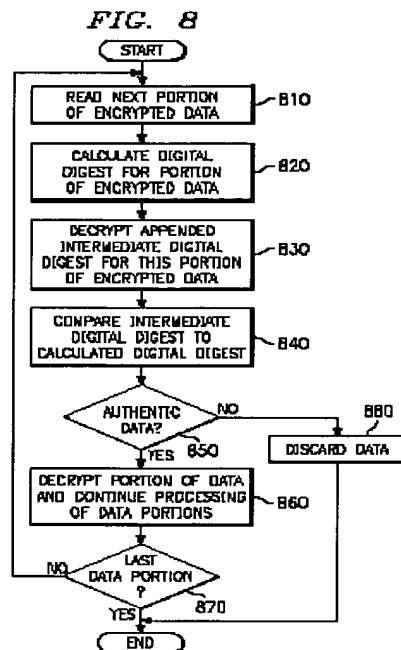
received with the re-transmitted data is compared with the stored received CRC that corresponds to the stored computed CRC which matched the newly-computed CRC. If these two received CRCs also match, then the receiver is deemed to be out of synchronization with the transmitter, and decryption site returns a resynchronization request to the transmitter in plain text. (*emphasis added*).

Weiss, Column 4, Line 63-Column 5, Line 63

Thus, Weiss is unambiguous that a CRC calculated from an encrypted data block or message is appended to the message and transmitted therewith. Moreover, Weiss clearly describes comparison of the "CRC received with... a data block" and the CRC "computed over that data block." Thus, the decryption methodology described by Weiss is performed on a block comprising encrypted data and an appended CRC computed from the data block. That is, the data package decrypted in the system described by Weiss comprises only a data block and appended CRC. Thus, Weiss clearly fails to describe, suggest, or otherwise allude to decryption of a "data package" comprising a "plurality of encrypted data portions" and a corresponding "plurality of encrypted intermediate digital digests." Particularly, Weiss fails to describe or suggest "reading an encrypted data portion" from the "plurality of data portions" of a data package as the data package described by Weiss only includes a single data block and CRC calculated therefrom. Thus, Weiss additionally fails to describe a methodology of calculating a digital digest for the "encrypted data portion" of a "plurality of encrypted data portions." Moreover, Weiss fails to describe a methodology of decrypting an intermediate digital digest "corresponding to the encrypted data portion from the plurality of intermediate digital digests" in a data package as only a single CRC is included in the message or data block described by Weiss. Consequently, Weiss additionally fails to describe or suggest a methodology of authenticating the encrypted data portion "of the plurality of data portions" based on a comparison of the "decrypted intermediate digital digest" of the "plurality of intermediate digital digests" with the "calculated digital digest." Accordingly, Weiss is thoroughly insufficient to anticipate the present invention as recited in claim 4.

As described in the present application, a method for decrypting an encrypted data package including a plurality of encrypted data portions and corresponding plurality of encrypted intermediate digital digests includes reading an encrypted data portion from the plurality of encrypted data portions. A digital digest is calculated from the read

encrypted data portion. An intermediate digital digest of the plurality of digital digests that corresponds with the read encrypted data portion is then decrypted. The encrypted data portion is then authenticated by comparing the decrypted intermediate digital digest with the calculated digital digest. For example, Figure 8 of the subject application shows the following:



As can be seen, a portion of the data message is read (step 810) and a digital digest for the read encrypted data portion is calculated (step 820). An intermediate digital digest corresponding to the encrypted data portion read at step 810 is then decrypted (step 830), and is compared with the decrypted intermediate digital digest. If the data is authenticated, the process repeats to read the next data portion until all encrypted data portions of the data message have been read and authenticated (See subject application, Page 4, Lines 10-19; Page 12, Lines 13-20 and Lines 24-27; and Page 14, Lines 6-19 and Lines 21-28).

Amended independent claims 14 and 24 recite similar features as claim 4 and were rejected with the same rationale applied to claim 4. Therefore, the same distinctions between Weiss and the claimed invention in claim 4 apply for these claims. For the reasons described above, Weiss does not contain all elements of independent claims 4,

14, and 24. Hence, Weiss fails to anticipate the present invention as recited in claims 4, 14, and 24. Consequently, it is respectfully urged that the rejection of claims 4, 14, and 24 under 35 U.S.C. § 102(b) in view of Weiss has been overcome.

Since claims 7-10 depend from claim 4, claims 17-20 depend from claim 14, and claims 27-30 depend from claim 24, the same distinctions between Weiss and the claimed invention in claims 4, 14, and 24 apply for these claims. Additionally, claims 7-10, 17-20, and 27-30 claim other additional combinations of features not suggested by the reference.

Consequently, it is respectfully urged that the rejection of claims 4, 7-10, 14, 17-20, 24, and 27-30 under 35 U.S.C. § 102(b) in view of Weiss has been overcome, and such a notice is respectfully requested.

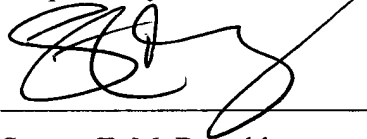
II. Conclusion

It is respectfully urged that the subject application is patentable over Weiss and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: December 21, 2004

Respectfully submitted,



Steven T. McDonald
Reg. No. 45,999
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Agent for Applicants



AUS920010388US1

McBrearty et al.

Apparatus and Method for Encrypting and
Decrypting Data with Incremental Data Validation

4/5

